Europ. J. Combinatorics (1989) **10**, 363–367

Cyclic Steiner Triple Systems with Cyclic Subsystems

KEVIN PHELPS, ALEXANDER ROSA AND ERIC MENDELSOHN

1. INTRODUCTION

A *Steiner triple system* of order v (briefly $STS(v)$) is a pair (V, B), where V is a v-set and B is a set of 3-subsets of V called *triples* such that each 2-subset of V is contained in exactly one triple. A *cyclic Steiner triple system* of order v (briefly $CTS(v)$), i.e. an STS with a regular cyclic automorphism group) can be thought of as a pair (Z_v, B), where Z_v is the additive group of integers modulo v fixing the set of triples B. An $STS(v)$ exists iff $v \equiv 1$ or 3 (mod 6), and a $CTS(v)$ exists iff $v \equiv 1$ or 3 (mod 6), $v \neq 9$ (see [5]). For a general reference on CTSs, see [2].

When $v = nu$, $n > 1$, $u > 1$, then the group of integers modulo v will have a (non-trivial) subgroup of order u and index n for each divisor u of v. In a similar fashion, one can define a cyclic subsystem of a $CTS(v)$ as having order u and index n, where (H, B_u) is the subsystem, and H is the subgroup of order u and index n which fixes B_u. A natural question asked, amongst others, by Peter Tannenbaum [6], is the following: What are the necessary and sufficient conditions for a $CTS(v)$ to contain a cyclic subsystem of order u and index n? The problem becomes more interesting when one realizes that the obvious necessary conditions—namely that u divides v, and that $u \equiv 1$ or 3 (mod 6), $u \neq 9$, $v \neq 9$—are not sufficient.

First we consider construction of such systems. The methods we use are variants of known composition methods for cyclic designs. Recent references on such methods include Colbourn and Colbourn [1] and Jimbo and Kuriki [3]. Some cases of the main results of this paper are probable consequences of previously published work and, to an extent, may be considered folklore. However, for the purposes of clarity and simplicity, our presentation will be self-contained.

2. EXISTENCE OF CYCLIC STEINER TRIPLE SYSTEMS WITH SUBSYSTEMS

Clearly, if there exists a cyclic Steiner triple system of order $v = nu$ having a cyclic subsystem of order u and index n, one of the following five cases must occur:

(1) $u \equiv 1$ or 3 (mod 6), $u \neq 9$ and $n \equiv 1$ (mod 6);
(2) $u \equiv 1$ (mod 6) and $n \equiv 3$ (mod 6), $n \neq 9$;
(3) $u \equiv 3$ (mod 6), $u \neq 9$ and $n \equiv 3$ or 5 (mod 6), $n \neq 3$;
(4) $u \equiv 1$ (mod 6), $u \geq 7$ and $n = 9$;
(5) $u \equiv 3$ (mod 6) and $n = 3$.

In this section we give constructions, which completely settle cases (1), (2), (3) and (4): we show that the above necessary conditions are sufficient in the sense that for all pairs (u, n) in cases (1)–(4), there exists a $CTS(nu)$ with a sub-$CTS(u)$ of index n. Case (5) is discussed in the next section, where we examine less obvious necessary conditions.

Given a $CTS(u)$ (Z_u, B'), we can form a sub-$CTS(u)$ of index n on the set $nZ_u = \{ni: i = 0, 1, \ldots, u-1\}$ having blocks $nb = \{nx, ny, nz\}$ for each $b = \{x, y, z\} \in B'$. In the following theorems we will always assume that the base blocks for such a system are present. In effect, we will be constructing cyclic group divisible designs with group size u and block size 3 on nu points.

A second construct, common to these proofs, is a *cyclic latin square* of order v,

0195-6698/89/040363 + 05 †02.00/0

denoted by $CLS(v)$. We will consider a $CLS(v)$ as a collection of v^2 ordered triples, L, on the set of integers modulo v such that if the triple $(x, y, z) \in L$ then the triple $(x+1, y+1, z+1) \in L$ (where the elements are reduced mod v). For our purposes, v will always be odd, and as any $CLS(v)$ will do, we can assume that $L = \{(x, y, z): z = (x+y)/2 \bmod v\}$.

THEOREM 2.1. *There exists a CTS(nu) having a cyclic subsystem of order u and index n if one of the following hold:*
(1) $u \equiv 1$ *or* $3 \pmod 6$, $u \neq 9$ *and* $n \equiv 1 \pmod 6$;
(2) $u \equiv 1 \pmod 6$ *and* $n \equiv 3 \pmod 6$, $n \neq 9$;
(3) $u \equiv 3 \pmod 6$, $u \neq 9$ *and* $n \equiv 3$ *or* $5 \pmod 6$, $n \neq 3$.

PROOF. Let (Z_u, B_u) be a $CTS(u)$, and let nB_u be the blocks of a cyclic subsystem of index n. These blocks will contribute $(u-1)/6$ or $(u-3)/6+1$ orbits to the $CTS(nu)$ (depending on the congruence class of u mod 6).

Case 1. $u \equiv 1$ or $3 \pmod 6$, $u \neq 9$ and $n \equiv 1 \pmod 6$. Let (Z_n, D) be a $CTS(n)$ and let L be a $CLS(u)$. For each orbit representative (base block) d of D and each orbit representative t of L, where $d = \{i, j, k\}$, $i < j < k$ and $t = (a, b, c)$, define a base block $\{i + an, j + bn, k + cn\}$. This gives $u(n-1)/6$ more base blocks for a total of $(u-1)/6 + u(n-1)/6 = (un-1)/6$ [or $(u-3)/6 + 1 + u(n-1)/6 = (un-3)/6+1$], which is the correct number of orbits. Any difference $d \equiv 0 \pmod n$ is contained in a base block of the sub-$CTS(u)$. For any difference $d \equiv s \pmod n$ there exists a unique base block in D containing s. Let us assume that $\{i, j, k\} \in D$ and $j - i \equiv s \pmod n$. Let us also assume that $d = s + rn$. Then for each $r = 0, 1, \ldots, u-1$ there exists a unique orbit representative (a, b, c) in L such that $b - a \equiv r \pmod u$. By our construction, there exists an orbit representative $\{i + an, j + bn, k + cn\}$ and clearly $d \equiv j + bn - (i + an) \pmod{un}$. Thus every difference is covered by at least one, and hence exactly one base block.

Case 2. $u \equiv 1 \pmod 6$ and $n \equiv 3 \pmod 6$, $n \neq 9$. The direct product of a $CTS(3)$ and a $CTS(u)$, $u \equiv 1 \pmod 6$ is well known to be a $CTS(3u)$ containing a sub-$CTS(u)$. Let L' denote the set of (base) blocks of such a system with those belonging to the sub-$CTS(u)$ deleted. For each base block $\{3a, 1+3b, 2+3c\}$ in L' construct a new base block $\{an, n/3 + bn, 2n/3 + cn\}$ (i.e. multiply each base block by $n/3$). These base blocks will contain every difference $d \equiv n/3 \pmod n$ exactly once. The construction now proceeds as in Case 1 for the remaining base blocks of a $CTS(n)$ (excluding the short orbit) and the orbit representatives of a $CLS(u)$.

Case 3. $u \equiv 3 \pmod 6$, $u \neq 9$ and $n \equiv 3$ or $5 \pmod 6$ but $n \neq 3$. Let L be a $CLS(u/3)$. Let (Z_{3n}, T) be a $CTS(3n)$. For each base block $\{a, b, c\}$, $a < b < c$ (excluding the short orbit $\{0, n, 2n\}$) and each orbit representative $\{i, j, k\} \in L$, form the base block $\{a + 3in, b + 3jn, c + 3kn\}$. This gives $((3n-3)/6)(u/3)$ base blocks which, when added to the $(u-3)/6+1$ base blocks of the sub-$CTS(u)$, gives $(un-3)/6+1$ base blocks—the correct number. Again, the differences $d \equiv 0 \pmod n$ are covered by the base blocks in the sub-$CTS(u)$. The remaining differences can be expressed in the form $s + 3rn$. Again, there exists a base block in T, and one in L, containing the differences s and r, respectively. Hence any difference is covered at least once, and therefore exactly once. □

We solve the next case by different methods.

THEOREM 2.2. *Let* $v = 9u$, *where* $u \equiv 1 \pmod 6$, $u \geq 7$. *Then there exists a CTS(v) containing a cyclic subsystem of order u and index* 9.

Before proving Theorem 2.2, we need a few auxiliary results. Write $u = 6t + 1$; then $v = 54t + 9$.

For any integer $t \geq 1$, let

$$A_t = \{1, 2, \ldots, 27t + 4\} \backslash \{9, 18, \ldots, 27t\} \backslash \{18t + 3\};$$

in other words, A_t is the set of all natural numbers not exceeding $27t + 4$ from which all multiples of 9 and one single extra value $18t + 3$ have been deleted. Clearly, $|A_t| = 24t + 3$.

Consider the following Heffter-type difference problem (note the resemblance to the two Heffter's difference problems, cf. [2]).

HP(t): Partition A_t into $8t + 1$ triples (a_i, b_i, c_i), $i = 1, 2, \ldots, 8t + 1$, such that for each i, either $a_i + b_i = c_i$ or $a_i + b_i + c_i \equiv 0 \pmod{54t + 9}$.

LEMMA 2.3. *If there exists a solution to HP(t) then there exists a CTS(v) with a cyclic sub-STS(u).*

PROOF. Take the triples (a_i, b_i, c_i) to be the difference triples associated with the $8t + 1$ orbits of a $CTS(v)$. If (d_i, e_i, f_i), $i = 1, 2, \ldots, t$, are difference triples associated with *any* $CTS(u)$, take the triples $(9d_i, 9e_i, 9f_i)$, $i = 1, 2, \ldots, t$, to be the difference triples associated with further t orbits of a $CTS(v)$. Finally, adjoin the short orbit with the difference triple $(18t + 3, 18t + 3, 18t + 3)$. □

Consider now the following Skolem-type (cf. [2]) partition problem:

SP(t): Partition the set B_t into $8t + 1$ pairs (p_r, q_r), $r \in \{1, 2, \ldots, 9t + 1\} \backslash \{9, 18, \ldots, 9t\}$, with $q_r - p_r = r$.

Here $B_t = \{9t + 2, 9t + 3, \ldots, 27t + 5\} \backslash \{9t + 9, 9t + 18, \ldots, 27t\} \backslash \{18t + 3, 27t + 4\}$. Clearly, $|B_t| = 16t + 2$.

LEMMA 2.4. *If there exists a solution to SP(t) then there exists a solution to HP(t).*

PROOF. Let $\{(p_r, q_r): r \in \{1, 2, \ldots, 9t + 1\} \backslash \{9, 18, \ldots, 9t\}\}$ be a solution to $SP(t)$. Let r^* be the index such that $q_{r^*} = 27t + 5$. Then

$$\{(r, p_r, q_r): r \in \{1, 2, \ldots, 9t + 1\} \backslash \{9, 18, \ldots, 9t\}, r \neq r^*\} \cup \{(r^*, p_{r^*}, q_{r^*} - 1)\}$$

is a solution to $HP(t)$. Indeed, for all $r \neq r^*$ we have $r + p_r = q_r$. Since $q_{r^*} = 27t + 5$, we also have $r^* + p_{r^*} = 27t + 5$, and so $r^* + p_{r^*} + (q_{r^*} - 1) = 54t + 9$. □

Thus in order to prove Theorem 2.2, all we have to do is to show that there exists a solution to $SP(t)$ for all $t \geq 1$.

LEMMA 2.5. *For any integer $t \geq 1$ there exists a solution to SP(t).*

PROOF. The proof proceeds by induction on t. For $t = 1$, a solution to $SP(1)$ is

$$(13, 14), \quad (17, 20), \quad (11, 16), \quad (12, 19),$$
$$(26, 28), \quad (25, 29), \quad (24, 30), \quad (15, 23), \quad (22, 32)$$

(the first row contains pairs with odd differences 1, 3, 5 and 7, and the second row pairs

with even differences 2, 4, 6, 8 and 10). For $t = 2$, a solution to $SP(2)$ is

$$(49-i, 50+i), \quad i = 0, 1, 2, 3, 5, 6, 7, \quad (24, 41), \quad (40, 59),$$
$$(31, 33), \quad (28, 32), \quad (23, 29), \quad (22, 30), \quad (25, 35), \quad (26, 38), \quad (20, 34), \quad (21, 37)$$

(again, the first row contains pairs with odd differences 1, 3, 5, 7, 11, 13, 15, 17 and 19, and the second row contains pairs with even differences 2, 4, 6, 8, 10, 12, 14 and 16).

A solution $\{(p_r, q_r)\}$ to $SP(t)$ will be said to have property P if the union of all pairs (p_r, q_r) with $r \equiv t \pmod 2$ covers all elements of the set B_t that are less than $18t+3$, except for $9t+6$. Note that our solutions to $SP(1)$ and $SP(2)$ above have property P.

Assume now that we have obtained, for a fixed $t \geq 3$, a solution $\{(\bar{p}_r, \bar{q}_r)\}$ to $SP(t-2)$ with property P. We are going to construct a solution $\{(p_r, q_r)\}$ to $SP(t)$ with property P.

The pairs (p_r, q_r) for r such that $r \not\equiv t \pmod 2$ (i.e. for r of parity opposite to that of t) are given by:

$$(18t+5+i, 27t+4-i) \qquad \text{for } i = 1, 2, \ldots, \lfloor (9t-2)/2 \rfloor, \ i \not\equiv 4 \pmod 9;$$
$$(9t+6, 18t+5) \qquad \text{(difference } 9t-1);$$
$$(18t+4, 27t+5) \qquad \text{(difference } 9t+1).$$

Note that the union of all these pairs covers all elements of the set B_t that are greater than $18t+3$, and also one extra value $9t+6$.

The pairs (p_r, q_r) for r such that $r \equiv t \pmod 2$ are of two kinds. The pairs with 8 largest differences, i.e. with differences $9t-16, 9t-14, \ldots, 9t-2$, are given by:

$$(9t+15, 18t-1), \quad (9t+10, 18t-4), \quad (9t+7, 18t-5), \quad (9t+4, 18t-6),$$
$$(9t+5, 18t-3), \quad (9t+8, 18t+2), \quad (9t+2, 18t-2), \quad (9t+3, 18t+1).$$

The remaining pairs with differences of the same parity as t are obtained from *all* pairs with differences of the same parity in a solution to $SP(t-2)$. These pairs will be $\{(\bar{p}_r + 27, \bar{q}_r + 27): r \equiv t \pmod 2\}$.

It is somewhat tedious but straightforward to verify that the union of all pairs with r having the same parity as t covers all elements of the set B_t that are less than $18t+3$, except for $9t+6$. Thus we have constructed a solution $\{(p_r, q_r)\}$ to $SP(t)$ which, moreover, has property P. □

PROOF OF THEOREM 2.2. Use Lemmas 2.5, 2.4 and 2.3 successively. □

3. Further Necessary Conditions

We now consider the last case (5), namely the existence of $CTS(9v)$ containing a cyclic subsystem of order $3v$ and index 3. Such systems cannot exist. We present a proof which is based on the arguments of [4]:

THEOREM 3.1 [4]. *There does not exist any $CTS(3u)$ having a cyclic subsystem of order $u \equiv 3 \pmod 6$ (and index $n = 3$).*

PROOF. Let $u = 3v$, and consider any $CTS(9v)$ containing a sub-$CTS(3v)$. Any difference $d \equiv 0 \pmod 3$ is covered by a base block of the sub-$CTS(3v)$. Any other orbit has a base block of the form $\{0, 3a+1, 3b+2\}$, where the differences are $3a+1$, $3(b-a)+1$, and $3(-b-1)+1$. Each difference mod $3v$ can be written as $3x+1$ for some $x = 0, 1, \ldots, v-1$. Hence each of the $v/3$ base blocks would contain

three distinct elements a, $b-1$, $-b-1$ (mod v), which add up to -1 (mod v) (i.e. $a+b-a+(-b-1)\equiv -1 \pmod{v}$). Hence $\sum_{x=0}^{v-1} x \equiv -1 \pmod{v}$. But $\sum_{x=0}^{v-1} x = v(v-1)/2 \equiv 0 \pmod{v}$ since v is odd, a contradiction. □

Acknowledgements

The authors would like to thank Luc Teirlinck for many helpful comments. The research of the second and third authors was supported by NSERC Canada Grants No. A7268 (A.R.) and No. A7681 (E.M.).

References

1. M. J. Colbourn and C. J. Colbourn, Recursive constructions for cyclic block designs, *J. Statist. Plann. Infer.* **10** (1984), 97–103.
2. M. J. Colbourn and R. A. Mathon, On cyclic Steiner 2-designs, *Ann. Discr. Math.* **7** (1980), 215–253.
3. M. Jimbo and S. Kuriki, On a composition of cyclic 2-designs, *Discr. Math.* **43** (1983), 249–255.
4. R. Mukerjee, M. Jimbo and S. Kageyama, On cyclic semi-regular group divisible designs, in *Designs and Graphs, Proceedings* (R. Fuji-Hara, ed.), Lect. Note Res. Inst. Math. Sci. Kyoto Univ. 587 (1985), pp. 16–31.
5. R. Peltesohn, Eine Lösung der beiden Heffterschen Differenzenprobleme, *Compositio Math.* **6** (1939), 251–257.
6. P. Tannenbaum, personal communication.

Received 20 July 1987

Kevin Phelps
Department of Algebra, Combinatories and Analysis, Auburn University, Auburn, Alabama 36849, U.S.A.

Alexander Rosa
Department of Mathematics and Statistics, McMaster University, Hamilton, Ontario, Canada L8S 4K1
and
Eric Mendelsohn
Department of Mathematics, University of Toronto, Toronto, Ontario, Canada M5S 1A4